Workshop on
Biometrics and E – Authentication Over Open Networks

Stephan Kent
Chief Scientist- Information Security
BBN Technologies

10 Moulton Street
Cambridge, MA 02139
Phone: 617.873.3988. kent@bbn.com

Topic: Biometrics: A System Security Perspective

Abstract: Most discussions of biometric technologies focus on the accuracy or security of specific biometrics or implementations thereof. This presentation examines system security issues and privacy concerns associated with use of biometric authentication in a technology independent fashion. The analysis notes that biometric authentication offers a very limited set of security functions, by itself. Biometrics provide only an initial authentication capability that usually needs to be converted into a cryptographic representation of user identity, to address the wide range of computer applications that require authentication as an input to access controls or for communication security purposes. Moreover, claims of the security superiority of biometric authentication are often made without adequate characterization of the threat environment. This analysis suggests that biometrics are best employed for local, not remote, authentication of users, to bind users to cryptographic keys for authentication.

Biography: During the last two decades, Dr. Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols secure e-mail technology, multi-level secure (X.500) directory systems, public-key certification authority systems, and key recovery (key escrow) systems. His most recent work focuses on public-key certification infrastructures, security for Internet routing, very high speed IP encryption, and high assurance cryptographic modules.

Dr. Kent served as a member of the Internet Architecture Board (1983-1994), and chaired the Privacy and Security Research Group of the Internet Research Task Force (1985-1998), both now under the auspices of the Internet Society. He chaired the Privacy Enhanced Mail (PEM) working group of the Internet Engineering Task Force (IETF) from 1990-1995 and co-chairs the Public Key Infrastructure Working Group (1995-). He is the primary author of the "core" IPsec standards. He served on the board of the Security Research Alliance and on the board of directors of the International Association for Cryptologic Research.

Dr. Kent chaired the committee on Authentication Technologies and Their Privacy Implications, for the Computer Science and Telecommunications Board (CSTB) of the National Research Council (2001-2003). He was a member of the CSTB-NRC Information Systems Trustworthiness Committee (1996-98), which produced the "Trust in Cyberspace" report. Other NRC service includes the committee on Rights and Responsibilities of Participants in Networked Communities (1993-94), the Technical Assessment panel for the NIST Computer Systems Laboratory (1990-1992 & 2000-2005), and the Secure Systems Study Committee (1988-1990). The U.S. Secretary of Commerce appointed Dr. Kent as chair of the Federal Advisory Committee to Develop a FIPS for Federal Key Management Infrastructure (1996-98).

The author of two book chapters and numerous technical papers on network security, Dr. Kent has served as a referee, panelist and session chair for a number of conferences. Since 1977 he has lectured on the topic of network security on behalf of government agencies, universities, and private companies throughout the United States, Europe, Australia, and the Far East. Dr. Kent received the B.S. degree in mathematics, summa cum laude, from Loyola University of New Orleans, and the S.M., E.E., and Ph.D. degrees in computer science from the Massachusetts Institute of Technology. He is a Fellow of the ACM and a member of the Internet Society and Sigma Xi.